HIT Policy Committee: NHIN Workgroup Planning Document

Authentication Hearing Overview

January 7, 2010

Testimony of SAFE-BioPharma Association

Presented by Mollie Shields Uehling
President and CEO

Introduction:

SAFE-BioPharma Association (Signatures and Authentication for Everyone) was established in 2005 by the world's leading research-based biopharmaceutical companies to develop and maintain an interoperable digital identity and signature standard which would help their business and regulatory processes become fully electronic. The resulting benefit is a single, interoperable digital identity which 1) reduces costs associated with multiple identities and credentials, 2) decreases cycle times, 3) allows for more easily searchable data/information, 4) increases information security and reduces fraud, 5) supports privacy and confidentiality per U.S. and EU regulations, and 6) greatly reduces the use of paper and associated costs in healthcare and life science processes.

The SAFE-BioPharma standard has the following characteristics:

- recognized and accepted by regulatory authorities including the US Food and Drug Administration (FDA) and the European Medicines Agency (EMEA).
- meets HIPAA and European Union data privacy requirements
- meets stringent European Union digital signature requirements
- is vendor and technology neutral
- is interoperable with the U.S. Government identity trust system
- comprises a system of governance and operational policies that every member, issuer, and participant is bound to through contract. Any possible dispute is mediated or arbitrated by the London Court of International Arbitration and not a court of law.

SAFE-BioPharma Association is a non-profit 501(c)6 organization with three major functions: 1) development and evolution of the standard; 2) education and advocacy for an interoperable identity standard, and 3) collaboration with the commercial sector a) to develop processes and technologies that streamline the process of obtaining and using a digital identity and b) to certify products and applications that are compliant with the SAFE-BioPharma standard.

As a collaborative consortium, SAFE-BioPharma's members participate in and provide direction through a highly engaged Board of Directors, Policy Approval Authority, and several Working Groups.

The SAFE-BioPharma community has conducted a number of credentialing pilots with physicians and clinicians. These pilots have led to significant changes to the standard and to major improvements in the identity proofing, credentialing, and digital signing processes.

The SAFE-BioPharma standard rests on a foundation of existing federal guidance and specifications related to identity trust and digital signature standards, principally OMB-04-04, OMB-05-05, NIST SP 800-63, and FIPS 201. SAFE-BioPharma's standard for digital certificates meets Internet Engineering Task Force x509, V3 and RFC 3647 Internet x.509 PKI Certificate Policy and Certification Practices Framework.

These are the same standards used by the U.S. Government and a growing network of cyber-communities which, due to their interoperability, allow different communities to trust the digital identities of participants in other sectors. The U.S. Government (GSA), Certipath (the aerospace and defense industry), the Higher Education Bridge Certificate Authority, and SAFE-BioPharma Association recently established The 4BF (The Four Bridges Forum) to raise awareness of this network of cyber-communities and to encourage use of these interoperable digital credentials across their respective trust bridges.

SAFE-BioPharma Association is pleased to have the opportunity to respond to the HIT Policy Committee NHIN Workgroup questionnaire below. The U.S. Government has a well-developed set of interoperable identity management standards under the purview of the Federal CIO Council's Identity, Credential and Access Management Sub-Committee and its Federal Public Key Infrastructure Policy Authority Work Group. This trust system is used by millions of government workers and contractors. It is supported by an expanding number of commercial providers. It is the common platform for a growing network of cyber-communities (e.g. The 4BF). The trust level of individual credentials is determined by risk assessment. The system meets the NHIN's privacy, security and confidentiality requirements. Most importantly, the trust system is scalable.

SAFE-BioPharma Association recommends that the U.S. Government extend the existing interoperable, vendor- and technology-neutral identity standards and processes to the NHIN. These standards are robust and provide the confidence needed to exchange sensitive health information electronically among trusted parties. Coupled with the existing user base, use of these existing standards will spur the growth and evolution of the NHIN.

Questions:

1. What trust problems are you trying to solve and for what range of users (e.g. organizations, individuals, health care professionals, consumers)? Please provide some quantitative data if possible to characterize your user base (e.g., percentage or number of each type).

The SAFE-BioPharma digital identity and signature standard was developed to provide the biopharmaceutical and healthcare sectors with a trust framework for authentication. The standard also provides a digital signature capability which is uniquely linked to the identity of the signer, is non-repudiable, provides record integrity, and can be validated both at the time of signing and subsequently. SAFE-BioPharma's mission is to facilitate the transformation of the healthcare and biopharmaceutical sectors to fully electronic business processes and to have many implementation options available to Members.

The early uses of the standard were for R&D and regulatory filings. The standard has and continues to expand to many other areas including physician signatures on medical diagnostics, purchasing and contracts by a Hospital Group Purchasing Organization (GPO), review and approval of medical promotional materials, partner/alliance management, IT support from foreign-based firms, records management, and legal signatures.

SAFE-BioPharma credentials are held by employees of biopharmaceutical companies, contract research organizations, clinical investigators and their staffs, contractors in the healthcare supply chain, physicians, outsourced IT providers, contractors, and others.

Because there are a number of cross-certified issuers, SAFE-BioPharma does not maintain a directory of the total universe of SAFE-BioPharma-compliant credential holders. The network of interoperable communities (U.S. Government, Certipath and SAFE-BioPharma) counts in the millions.

2. Who pays for the solution, implementation, processes and support for your approach? What factors contribute to the total cost of ownership of the technologies, including process costs? What are the implications to widespread deployment?

The SAFE-BioPharma standard accommodates Basic Assurance and Medium Assurance Hardware, Software and Digital Roaming credentials. It provides for identity proofing 1) through an on-line process accessing antecedent data, 2) by notary or 3) by a trained Trusted Agent.

The standard has expanded over the past several years as a result of a series of pilots providing credentials to physicians and to others. The standard will continue to evolve based on continuing pilot and implementation experience.

.SAFE-BioPharma Association works with the commercial sector to provide cross-certified certificate issuance services to the SAFE-BioPharma community. The association also works with individual members to establish their own internal infrastructures. In addition, SAFE-BioPharma Association manages an identity-proofing and credentialing service as a shared service for its members.

Costs depend on a variety of factors including the number of users, the type of identity-proofing process, and the type of credential. The range currently is between $35 and $66 per year per user for a Medium Assurance software credential. Association membership is a prerequisite for participation.

The fundamentals enabling widespread deployment are in-place. There are existing standards and processes that are recognized and used by both the federal government and the private sector; there are a variety of competitive commercial solutions and providers to support implementations; and there are existing interoperable communities of millions of credential holders of which the NHIN could become a part.

The most rapid path to widespread adoption is building awareness of the importance of strong identity management as fundamental to security, privacy and confidentiality in an electronic world. This means a change in the mindset to move beyond user name/password for access to and exchange of sensitive healthcare information. It also means community adoption of a flexible, robust interoperable digital identity standard.

3. Directory services often support some certificate authority or other authentication mechanism. As you look more broadly at the architecture, how do your approaches work with such directory services?

SAFE-BioPharma Association provides an identity credential fully aligned with the Federal PKI Policy Authority (FPKIPA) and cross-certified with the Federal Bridge Certificate Authority (FBCA). These credentials are for primary use for identity authentication and digital signatures.

The status and validity of these credentials/certificates are verified or validated in real-time, upon each use.

SAFE-BioPharma holds the position that authentication and authorization are separate and distinct phases of the process of granting access to information. While multiple sources may provide authentication credentials, only the owner or custodian of information should manage the authorization phase.

There are emerging Identity Service Providers -- organizations that include additional information about the certificate holder. This information generally includes authorizations/permissions/privileges, offered by the certificate or credential holder's assurance level and/or role. These additional capabilities, when consistent throughout a community, become known as a federated identity. SAFE-BioPharma works with the Federal and European governments and appropriate standards organizations (e.g., Kantara, HL7, CDISC and others) to maintain alignment, as approaches to authorizations emerge and coalesce.

4. Does your approach support a delegated authentication model where there is an authorized registrar that issues the authentication credentials to individuals? If so, how? Are there implications for interoperability in this scenario?

The SAFE-BioPharma standard supports delegated authentication in three ways: The first is via commercial cross-certified Certificate Authorities. We also support members in establishing internal services. Lastly, SAFE-BioPharma operates a Registration Authority System (RAS) as a shared service. Commercial cross-certified issuers include Citibank, Chosen Security, IdenTrust, TranSped, and Verizon Business. Companies which have built their own infrastructures and cross-certified them are Bristol-Myers Squibb and Johnson & Johnson. There are currently several additional commercial providers in the cross-certification process. Each cross-certified issuer has the flexibility to establish multiple types of identity-proofing processes including the on-line antecedent process, notary, and Trusted Agent (delegated).

Working with the physician community over the past several years has prompted several adjustments that make the SAFE-BioPharma standard suitable for healthcare processes and culture. These changes include improvements to identity-proofing, credentialing and signing processes. One innovation -- an on-line antecedent identity proofing process -- allows physicians and other healthcare professionals to obtain a digital identity in about 15 minutes. This on-line process, developed in collaboration with the FPKIPA/CPWG and meeting the FBCA CP, can check the medical license information of applicants. If an individual is unable to use the on-line process, a notary from the National Notary Association can visit the individual's home, office or other place of convenience to perform the identity proofing. In another innovation, SAFE-BioPharma is now in the process of piloting a truly "zero footprint" token, eliminating the desktop driver download needed for strong, two-factor authentication.

5. What should be the role of government? Where can rapid action address common concerns or limitations of trust?

The U.S. government has a well-developed and broadly accepted set of interoperable identity management standards and processes under the purview of the Federal CIO Council's Identity, Credential and Access Management Sub-Committee and its Federal Public Key Infrastructure Policy Authority Work Group. This trust system is used by millions of government workers and contractors; it is supported by an expanding number of commercial providers; it is the common platform for a growing network of cyber-communities (e.g., The 4BF); the trust level of individual credentials is determined by risk assessment; the system meets the NHIN's privacy, security and confidentiality requirements; and, most importantly, it has proven scalable.

SAFE-BioPharma Association recommends that the U.S. government extend these interoperable, vendor- and technology-neutral standards and related identity-proofing processes to the NHIN. These standards and proven processes provide the confidence needed to exchange sensitive health information among trusted parties. Its effect will spur the growth and evolution of the NHIN.